024044

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number
WO 01/03401 A1

(51) International Patent Classification[7]: H04L 29/06, H04Q 3/00

(21) International Application Number: PCT/EP99/04624

(22) International Filing Date: 2 July 1999 (02.07.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: NOKIA NETWORKS OY [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: WALLENIUS, Jukka [FI/FI]; Keinutie 8 G 41, FIN-00940 Helsinki (FI).

(74) Agents: TRÖSCH, Hans-Ludwig et al.; Tiedtke-Bühling-Kinne, Bavariaring 4, D-80336 München (DE).

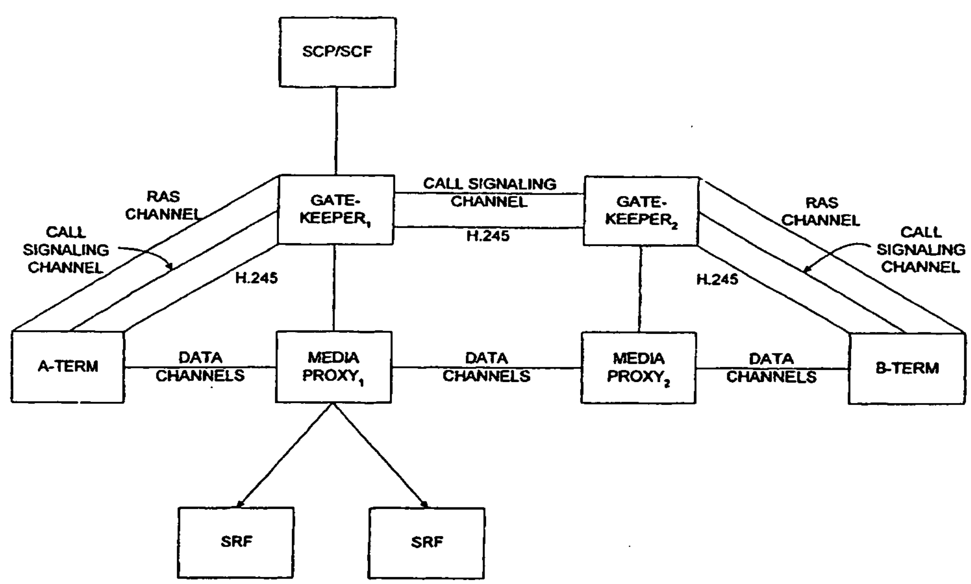
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROVIDING CONNECTION CONTROL FOR SEPARATE LOGICAL CHANNELS IN H.323 MULTIMEDIA



(57) Abstract: According to the present invention, a connection control for separate media components forming a multimedia stream transferred between two end-points each located in a network system is provided. For this purpose, media component control signaling between the end-points is monitored by routing means. Then, the routing means inform control means about separate media components, recognize the separate media components associated with a call between the two end-points and apply a connection control issued by the control means to the separate media components.

WO 01/03401 A1

THIS PAGE BLANK (USPTO)

10/018864
13 Rec'd PCT/PTO 17 DEC 2001

TITLE OF THE INVENTION

Providing connection control for separate logical channels in H.323 multimedia.

FIELD OF THE INVENTION

The present invention relates to a method and a system for providing a connection control for separate media components forming a multimedia stream which is transferred between two end-points each located in a network system.

It is to be noted that, throughout the present invention, IN (Intelligent Network) designates any solution in which a call, connection or session processing node contacts a service control function (SCF) which issues instructions to the respective node. The contact to the service control function is based on a trigger information stored in the respective nodes, or downloaded there from external servers such as location registers. The trigger information may specify situations in the course of a call, connection or session handling. The service control function may be internally distributed. Moreover, the corresponding IN protocol could be any protocol between a controlling entity, such as a service control function, responsive to triggering from a call, and a session or connection node. The IN protocol may for example be an object oriented interface where the operations are object methods or invocations.

Further, it is to be noted that throughout the present invention H.245 designates any signaling used in media component establishment, modification and release. In addition, according to the present invention, the term gatekeeper designates any node responsible for call routing

and control and optionally other telephone switch type of functionalities like charging.

BACKGROUND OF THE INVENTION

The ITU-T Recommendation H.323 specifies multimedia conferencing over packet networks. According to H.323 it is possible to have several media components in a multimedia call or session. These separate media components forming a multimedia stream are handled end-to-end outside the multimedia call establishment which is done using Q.931 signaling between a gatekeeper, a terminal and an external network such as PSTN (Public Switched Telephone Network). The gatekeeper is an H.323 entity which provides services like address translation and control access for network elements such as terminals and gateways. The media components are established using the H.245 signaling from end-to-end.

Similarly, in the IETF (Internet Engineering Task Force) IP (Internet Protocol) telephony protocol SIP (Session Initiation Protocol) the establishment and modification of multimedia streams is performed using end-to-end signaling. Its SDP (Session Description Protocol) definitions within the INVITE method inviting a user to a call are treated as H.245 signaling even though not intercepted from a media proxy, but from a SIP call processing server.

If current IN (Intelligent Network) architectures are applied to the gatekeeper, the gatekeeper is able to control the call routing and handling using known INAP (Intelligent Network Application Protocol) operations. However, if the media stream is established directly between the endpoints as performed according to H.323 and SIP specifications, the media stream is outside the control of the gatekeeper and further the SCP (Service Control Point) having a Service Control Function (SCF). Using media gateway control

protocols, the SCP is able to control an entire media stream composed of one component such as G.711 encoded voice, but the separate media components from a multimedia stream are not visible for an SCP.

The media stream may be composed of several media components routed via different paths.

Similarly, the separate media components cannot be connected to external resources separately.

SUMMARY OF THE INVENTION

Therefore, it is an object of the present invention to provide services also for individual multimedia stream components.

According to a first aspect of the present invention, this object is achieved by a method for providing a connection control for separate media components forming a multimedia stream transferred between two end-points each located in a network system, comprising the steps of:

monitoring media component control signaling between the end-points;

informing control means about separate media components;

recognizing the separate media components associated with a call between the two end-points; and

applying a connection control issued by the control means to the separate media components.

According to a second aspect of the present invention, this object is achieved by a network system for providing a connection control for separate media components forming a multimedia stream transferred between two end-points, comprising:

routing means for monitoring media component control signaling between the end-points, informing control means about separate media components, recognizing the separate media components associated with a call between the two end-points, and applying a connection control issued by the control means to the separate media components.

According to the present invention, the routing means which may comprise call control means and media proxy means receive a media component control signaling message.

Moreover, the routing means may send a message to the control means and wait for a response from the control means. Further, the routing means which may comprise call control means and media proxy means may receive a message from the control means and send a modified component control signaling message from the call control means.

In addition, if the media component control signaling messages are routed via the media proxy means, the call control means may request report of media component related events from the media proxy means and the media proxy means may inform the call control means of the media component related events.

Furthermore, the multimedia stream may be routed via the media proxy means communicating with the call control means.

Moreover, the routing means may send a message from the call control means to the control means and wait for a response from the control means to the call control means.

Furthermore, the media component control signaling message may describe opening, closing or modifying a media component.

Further, the media component control signaling message may be in association with a call signaling message.

In addition, the media components associated with a call are recognized in the media proxy.

Finally, in order to provide connection control, the control means issue connection control requests to the call control means, the call control means issue connection control requests to the media proxy means and the media proxy means switch the media components in accordance with the connection control requests. The switching may involve media proxy switching IP packet payloads carrying a media component between an incoming and outgoing packet stream.

The connection control may not occur in all cases where the invention is applied. The indication of media component information to the control means without connection control may be beneficial to enforce for instance charging tariff determination in the control means.

In accordance with the present invention, media component related signaling (H.245) messages can be intercepted by the routing means to the control means. The messages can be modified and relayed further in accordance with the normal routing of the H.245 messages. In this way, the media component manipulations can be made invisible to the end-points. The control means can emulate an endpoint to the other endpoint. The separate multimedia stream components can be identified and switched separately by the proxy means.

In case SIP is used in a call processing node, the session description protocol definitions from the SIP INVITE method inviting a user to a call can be intercepted to the control means.

According to the present invention, the media component related detection points can be made into a separate media component statemodel which is parallel to the basic call statemodel. A connection view model of the separate media components and their states can be presented to the control means.

The present invention enables the use of specific IN services for separate multimedia stream components. Examples for such services are the control of a conversion loop, message modification and control of charging.

The terminal capability negotiations occurring during the call set-up can be intercepted by the routing means to the control means to enable the control means to modify the terminal capability information elements to reflect for example the conversion capabilities available via the conversion loops for the separate media components. The modified terminal capability information elements can be returned by the control means to the routing means to be relayed further in the continued terminal capability negotiations.

In the following, a preferred embodiment of the present invention will be described in connection with the accompanying drawing.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 shows an architecture of signaling between an IP network and an SC network with use of back-end services.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Fig. 1 shows an IP (Internet Protocol) network adopting H.323 signaling, which may communicate with an SN (Switched Circuit) Network like PSTN (Public Switched Telephone Network) to which mobile or fixed phones are connected.

H.323 specifies multimedia conferencing over packet networks like the IP network. A call using H.323 signaling is the point-to-point multimedia communication between two H.323 end-points, either direct or via gatekeeper(s) and/or MCs (Multipoint Controllers). The media mix in a call can consist of audio, video and data streams. Audio communication has to be supported, video and data are optional. Media can be added, dropped or replaced dynamically during a call.

According to H.323, even a two-party call is considered as being a special case of a multiparty conference.

In the IP network shown in Fig. 1, a gatekeeper (gatekeeper1 or gatekeeper2) connects to a terminal (A-term or B-term) via an RAS (Registration, Admission and Status) channel, a media proxy and another gatekeeper. The gatekeeper which is a H.323 entity of the IP network provides address translation and control access to the IP network for terminals, gateways and MCUs (Multipoint Control Units). The gatekeeper also provides other services to the terminals, gateways and MCUs such as bandwidth management and gateway location.

The call set-up signaling can also be relayed via the gatekeeper. Similarly, the H.245 control signaling can be routed via the gatekeeper. According to the present invention, the gatekeeper is also controlling one or more media proxies, via which all the data channels carrying the individual media components can be routed. The gatekeeper is able to instruct the media proxy to perform connections on these data channels. The data channels can be connected to

other nodes like SRFs, upon instructions from the gatekeeper. The connections can be created, modified and deleted.

The end-to-end multimedia stream may comprise several media components routed along different paths, but they have to be routed via a media proxy under the control of a gatekeeper to enable connection control as requested by the gatekeeper. The routing via media proxies can be implemented in several ways, the gatekeeper may modify the media component establishment signaling message parameters to reflect the routing of the media component via a media proxy. In this way the packet traffic comprising a media component can be routed to the media proxy from the adjacent end-points or media proxies. Alternatively, the routing of the media component via media proxies can be enabled by providing routing information to the end-points.

The media proxy is able to identify the separate media components from the multimedia stream. The media proxy can perform switching of the individual media components separately. The identification of the separate media components can be performed by labeling the IP packets associated with a given media component with specific labels in the sending node. Alternatively, the media proxy checks the IP packets for other identifying information such as RTP (Real Time Protocol) port numbers. This is required because the different media components may have the same source and destination IP addresses. The gatekeeper must provide the media proxy with information on each call and its associated media components as soon as they are known by the gatekeeper. This information includes information that enables the media proxy to identify the separate media components. In this way, the media proxy can execute the connection control instructions from the gatekeeper and perform switching.

Similarly, the gatekeeper can instruct the media proxy on required bandwidth to be allocated for the data channels. The packets associated with the data channels associated with gatekeeper1 processed calls are routed in the IP network via media proxy1.

According to an alternative embodiment of the present invention, the H.245 control signaling may also be routed via the media proxy.

According to the H.323 specification, several separate media components forming a multimedia stream are possible. These media components are established using H.245 end-to-end signaling. The H.245 signaling is adopted between two end-points or between an end-point and an MCU and provides plural functions such as capabilities exchange, opening and closing logical channels, flow control, media loop, etc.

According to SIP (Session Initiation Protocol), several separate media components forming a multimedia stream are as well possible. These media components are established using SIP INVITE methods and its responses carrying media component descriptions according to SDP (Session Description Protocol). These media component descriptions are contained in MIME (Multipurpose Internet Mail Extensions) format message bodies.

In case specific IN services of an SCP (Service Control Point) are to be used for the separate media components of the multimedia stream, the separate media components are to be made visible to the SCF.

Usually, each real-time media component is carried in a separate pair of uni-directional unreliable channels, one for each direction. A call with audio and video components therefore involves at least four logical channels. Data

traffic, however, uses a bi-directional reliable channel. Here, "reliable channel" means connection-mode transport, while "unreliable channel" refers to connectionless transport. In an IP-based scenario, this corresponds to TCP (Transport Control Protocol) and UDP (User Datagram Protocol), respectively.

Hence, the H.245 logical channels corresponding to the separate media components, respectively, must be made recognizable to the SCF.

Similarly, the existence of media components indicated in SIP messages must be made visible to the SCF.

According to the present invention, a method of implementing IN type control for the components of a multimedia stream is proposed. To this end, the states of the media component streams are modeled in the gatekeeper. If the H.245 control channel or its equivalent channel, which is used to open, close and modify media components, is routed via the media proxy or an equivalent node, the gatekeeper must be informed of each message affecting the states of the media components.

The modeling of the media component streams in the H.323 media proxy is done by monitoring the component specific H.245 signaling between the terminals or end-points of the communication. Similarly, an other media component control signaling like SIP INVITE methods can be monitored similarly to enable the modeling. An example for such a state model used for the media components is an IN CS-3 type of connection view model which is made visible to the SCF by the gatekeeper, possibly with media proxy assistance.

The state model according to the present invention includes detection points (DP) triggering messages which are sent to the SCF or SCP via the gatekeeper which has its own INAP

(Intelligent Network Access Protocol) for communicating with the SCP or via an own INAP interface of the media proxy.

Similarly, the invention enables the SCF to intercept logical channel descriptions from SIP methods like INVITE, to alter them and provide the modified description information to the gatekeeper.

Messages are triggered according to trigger criteria such as a digit string, cause value, specific origin, feature activation, nature of address or a combination thereof.

In accordance with this invention, the SCF can define detection point reporting criteria for the reporting of media component events signaling to the SCF. According to an embodiment of the present invention, the reporting criteria for detection points can define message types, message parameter values and parameter value ranges within a given message type. In most typical cases the H.245 messages like OpenLogicalChannel and CloseLogicalChannel can be reported to the SCF.

The reporting criteria can include logical operations such as AND, OR and NOT. For example, the reporting of media encodings not listed in the reporting criteria can be enabled.

According to the preferred embodiment of the present invention, the message type criterion can be omitted from the event report request, if the detection point identifies the message received. For instance, the SCF can set detection point reporting criteria on media component establishment message receipt in the gatekeeper (OpenLogicalChannel) with the criteria being such that the message indicates media types or encodings other than the ones listed by the SCF.

CLAIMS:

1.A method for providing a connection control for separate media components forming a multimedia stream transferred between two end-points each located in a network system, comprising the steps of:

monitoring media component control signaling between the end-points;

informing control means about separate media components;

recognizing the separate media components associated with a call between the two end-points; and

applying a connection control issued by the control means to the separate media components.

2. The method according to claim 1, wherein in the monitoring step call control means receive a media component control signaling message.

3. The method according to claim 1, wherein the informing step includes the steps of:

sending a message to the control means; and

waiting for a response from the control means.

4. The method according to claim 1, wherein the informing step includes the steps of:

sending a message to the control means;

waiting for a response from the control means;

receiving a message from the control means; and

sending a modified component control signaling message from call control means.

5. The method according to claim 2, wherein in the monitoring step, if the media component control signaling messages are routed via media proxy means, the call control means request report of media component related events from the media proxy

means, and the media proxy means inform the call control means of the media component related events.

6. The method according to claim 1, wherein the multimedia stream is routed via media proxy means communicating with call control means.

7. The method according to claim 1, wherein the informing step includes the steps of:

sending a message from call control means to the control means; and

waiting for a response from the control means to the call control means.

8. The method according to claim 2, wherein the media component control signaling message describes opening, closing or modifying a media component.

9. The method according to claim 2, wherein the media component control signaling message is in association with a call signaling message.

10. The method according to claim 6, wherein the media components associated with a call are recognized in the media proxy.

11. The method according to claim 10, further comprising a connection control step including the steps of:

issuing connection control requests from the control means to the call control means;

issuing connection control requests from the call control means to the media proxy means; and

switching the media components by the media proxy means in accordance with the connection control requests.

12. The method according to claim 11, wherein the switching step involves media proxy switching IP packet payloads carrying a media component between an incoming and outgoing packet stream.

13. A network system for providing a connection control for separate media components forming a multimedia stream transferred between two end-points, comprising:

routing means for monitoring media component control signaling between the end-points, informing control means about separate media components, recognizing the separate media components associated with a call between the two end-points, and applying a connection control issued by the control means to the separate media components.

14. The network system according to claim 13, wherein the routing means which comprise call control means and media proxy means receive a media component control signaling message.

15. The network system according to claim 13, wherein the routing means send a message to the control means and wait for a response from the control means.

16. The network system according to claim 13, wherein the routing means send a message to the control means, wait for a response from the control means, receive a message from the control means and send a modified component control signaling message from call control means.

17. The network system according to claim 14, wherein, if the media component control signaling messages are routed via the media proxy means, the call control means request report of media component related events from the media proxy means and the media proxy means informing the call control means of the media component related events.

18. The network system according to claim 13, wherein the multimedia stream is routed via media proxy means communicating with call control means.

19. The network system according to claim 13, wherein the routing means send a message from call control means to the control means and wait for a response from the control means to the call control means.

20. The network system according to claim 14, wherein the media component control signaling message describes opening, closing or modifying a media component.

21. The network system according to claim 14, wherein the media component control signaling message is in association with a call signaling message.

22. The network system according to claim 18, wherein the media components associated with a call are recognized in the media proxy.

23. The network system according to claim 22, wherein, for connection control, the control means issue connection control requests to the call control means, the call control means issue connection control requests to the media proxy means and the media proxy means switch the media components in accordance with the connection control requests.

24. The network system according to claim 23, wherein the switching involves media proxy switching IP packet payloads carrying a media component between an incoming and outgoing packet stream.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/04624

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04Q3/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 909 064 A (KOKUSAI DENSHIN DENWA CO LTD) 14 April 1999 (1999-04-14) page 3, line 31 -page 4, line 51; figures 1A,1B	1,13
A	US 5 717 859 A (YUNOKI HIDEO) 10 February 1998 (1998-02-10) column 3, line 8 - line 50	1,13

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 February 2000	08/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ströbeck, A

1

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/EP 99/04624

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RIZZETTO D ET AL: "A Voice over IP Service Architecture for Integrated Communications" IEEE INTERNET COMPUTING, vol. 3, no. 3, May 1999 (1999-05) - June 1999 (1999-06), pages 53-62, XP002131520 Piscataway, NJ, USA page 60, right-hand column, line 46 -page 62, left-hand column, line 27	1,13

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inten nal Application No
PCT/EP 99/04624

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0909064 A	14-04-1999	JP 11068851 A	09-03-1999
US 5717859 A	10-02-1998	JP 7264284 A	13-10-1995
		CN 1114810 A	10-01-1996
		GB 2287611 A,B	20-09-1995

A VOICE OVER IP SERVICE ARCHITECTURE for Integrated Communications

DANIELE RIZZETTO AND CLAUDIO CATANIA
Hewlett-Packard Laboratories

A novel architecture supports flexible integration of IP-based telephony services with legacy circuit-switched services by defining the means for convergence at the communications-control layer of the network, rather than the transport layer.

Voice over IP has paved the way for a global approach to designing communication service platforms, but the real driver is the convergence between heterogeneous communication network technologies. Schulzrinne[1] considered some of the problems arising from this convergence and described possible scenarios for the evolution of the current communication world. The integration needs of existing systems slow down the introduction of new technologies and communication tools. Integrating heterogeneous networks at the communication-control layer can speed up this process. Integrating the intelligent network (IN)[2] and the Internet is a key step in this direction.

This article advances a high-level abstraction for integrating IP-based telephony intelligent services with legacy circuit-switched telephony IN services. We do not propose new protocols; rather, we present a novel service architecture, its components, and their behavior. We focus on International Telecommunication Union Recommendation H.323 for VoIP[3] (see the sidebar "H.323: An Overview" on the next page) and its central network component, the gatekeeper. In particular, we describe the architectural design and findings of the Hewlett-Packard Laboratories Bristol (HPLB) gatekeeper, an experimental prototype implemented on top of an H.323 platform. We also describe a practical demonstration of interoperation between the Internet and the IN.

ARCHITECTURE RATIONALE

Our proposed architecture takes advantage of VoIP's flexibility by defining the means for convergence at the communications-control network layer, rather than the transport layer. The ever-growing availability of communication networks that offer similar functionality using different technologies suggests the need for a high-level abstraction to execute the services inde-

pendent of the user's network connection. Our approach defines a network-independent service environment into which different communication stacks can be plugged. Uncoupling the protocols from the platform is the first step toward convergence at the control layer.

With VoIP, communications services are more logically implemented in terminals than in centralized service components.[4] This is because IP terminals are far more powerful and intelligent than traditional telephones and provide better user interfaces. As the migration to IP terminals gets under way, more services will be implemented in devices at the edge of the network. Nevertheless, some services implement functionality that cannot run on the client side. Among them are call routing, directories, and services that suffer from the "always-on" problem of client end terminals, which stems from the fact that VoIP terminals are not always on and connected to a network. Our approach, although essentially server-based, acknowledges the "intelligence at the edge" vision and supports it by offering an entirely IP-based platform easily accessible by smart terminals.

Integrated service platforms must provide services that end users can easily access and configure.[5] The standardized access provided by IP is instrumental in achieving this goal, but the service model has to enable this capability. Our agent-based approach to provisioning communication services lets users modify the logic of their services and decide how service

H.323: AN OVERVIEW

H.323 is an ITU umbrella Recommendation for multimedia communications over local area networks (LANs) that do not provide a guaranteed quality of service (QoS)[1] (for a concise introductory tutorial see DataBeam's "A Primer on the H.323 Series Standard"[2]). The standard covers point-to-point communications and multipoint conferences. It addresses call control, multimedia management, bandwidth management, and interfaces between LANs and other networks.

Architecture

The Recommendations are still under development (H.323v2 was approved in January 1998), but some basic concepts are widely accepted. The architecture elements are

- *User terminals*. Terminals are the LAN client endpoints that provide real-time two-way communications.
- *Gateways*. GWs translate signaling and media streaming exchanged between H.323 and PSTN endpoints.
- *Multipoint control units*. MCUs enable conferencing.
- *Gatekeepers*. GKs are responsible for call authorization, address resolution, and bandwidth management. They intercept call signaling between endpoints and provide "signaling-based" advanced services.

Terminals, gateways, and MCUs are generically addressed as endpoints. GKs provide those services that cannot be decentralized and implemented by endpoints.

The Registration Admission Status (RAS) protocol is the key GK protocol. RAS messages are carried in User Datagram Protocol (UDP) packets exchanged between an endpoint and its GK. When an endpoint is switched on, it sends an RAS registration request (RRQ) to the GK. This message contains information such as terminal transport address, user alias, and E.164 telephone number. If the GK accepts the registration, it sends a Registration Confirm message (RCF); otherwise, it sends a Registration Reject (RRJ) message. The GK and its registered endpoints are called a zone.

Call Setup Life Cycle

The H.323 call setup life cycle can be split into three phases (named according to the protocol used):

RAS. To make a call, an H.323 endpoint sends an RAS Admission Request (ARQ) message to the GK. This message contains the destination alias, which is the name or phone number of the user to be contacted. The GK may grant permission for the call by sending back an Admission Confirm (ACF) message containing the actual transport address associated with the called party alias. The GK may also reject the request with an Admission Reject (ARJ) message for a variety of reasons, such as "not enough bandwidth" or "security violated." Therefore, during this phase the GK accomplishes three functions: address translation, call authorization, and bandwidth management.

Q.931. This phase is derived from ISDN end-to-end call setup signaling (SETUP, PROCEEDING, ALERTING, CONNECT) and provides the logical connection between the two endpoints—the calling party and the called party. In H.323, Q.931 is implemented on top of TCP.

H.245. During this phase, the two endpoints exchange capabilities. They agree on the nature of the information

objects will behave when reacting to events sent from the network and dialoguing with other entities involved in the communication session. A similar approach is the call management agent.[6]

Letting end users configure their own services requires careful analysis of the language used to implement them because badly programmed logic can harm the network's overall functionality. A well thought-out language that is user-friendly, can handle complex and advanced services, and can offer the appropriate reliability features required by communication networks has yet to be devised. Our proposal, while offering a simple rule-based language to program the service logic, implements peer-to-peer negotiation in the service platform among all the service objects of the parties involved in the communication session. We believe this approach solves the above-mentioned problem and takes a step beyond the traditional telephony world service model, in which the called party plays a dominant role in triggering and executing services.

SERVICE ARCHITECTURE

The main components of the service architecture are shown in Figure 1. The GK platform provides a high-level application programming interface (API) that implements an abstraction layer for executing services independent of the underlying networks. Each GK platform has a local service platform in which service objects are executed. A service object implements ser-

they will exchange through the media channel (audio, video, or data) and its format (for example, compression or encryption). H.245 is implemented on top of TCP.

After these three phases, the Real-Time Protocol/Real-Time Control Protocol (RTP/RTCP, running on top of UDP) media channels between the two endpoints are opened according to the capabilities exchanged, and the actual media communication starts. Data communications are based on the T.120 specification. During the call, dual-tone multifrequency (DTMF) touch tones are transmitted over the LAN through the H.245 User Input Indication message.

Call signaling can be routed through the GK or routed directly between the endpoints. RAS is, by nature, GK-routed. A GK can decide to route Q.931 and H.245 through itself, so that it can act as a proxy between endpoints. If the GK intercepts the signaling it can perform call management, maintaining a list of ongoing H.323 calls in order to keep endpoints' state or to provide information for the bandwidth management function. In any case, the media flows directly between endpoints because the GK is just a signaling entity and cannot be called.

New Features

H.323v2 uses the H.235 standard to address authentication, integrity, privacy, and nonrepudiation.

It has also introduced the Fast Connect procedure, which allows endpoints to expedite the exchange of terminal capabilities by encapsulating them in Q.931 messages, thus avoiding the slow H.245 negotiation.

Supplementary services have been defined by the H.450 series. H.450.1 is the signaling protocol between endpoints for the control of supplementary services; H.450.2 defines call transfer of an established call; and H.450.3 defines call diversion for implementing call forwarding unconditional, call forwarding busy, call forwarding no reply, and call deflection. New services can be introduced through the standardization of a new H.450.X series. The series puts in place signaling mechanisms to control services, but do not define how the logic behind them should be implemented.

Beyond Signaling

The Internet Engineering Task Force proposal for VoIP signaling is the Session Initiation Protocol.[3] SIP goes beyond the simple signaling of voice communications. It focuses on setting up generic communication sessions, separating this phase from channel allocation and media transmission. SIP uses the REGISTER message to register to a SIP server and the INVITE message to initiate a call. This message can be sent directly to a SIP client or SIP server, which is comparable to a H.323 GK. If the SIP server is a proxy server, it will route the call through itself; if it is a redirect server, it will redirect the call to the actual destination.

REFERENCES

1. ITU-T Rec. H.323, "Visual Telephone Systems and Equipment for Local Area Networks which Provide a Nonguaranteed Quality of Service," Geneva, Switzerland.
2. DataBeam Corp., "A Primer on the H.323 Series Standard," http://www.databeam.com/h323/h323primer.html.
3. M. Handley, H. Schulzrinne, and E. Schooler, "SIP: Session Initiation Protocol," Internet draft, IETF, Jan. 1999; work in progress.

vices for a particular user, who can modify and configure them at any time. For each user there is a service object stored in a home server, which is shared among several users. The server can be located anywhere in the network. When a user changes location, the local GK-service platform accepts the registration and downloads the user's service object from the home server in which the object is stored.

HOME SERVER

The home server contains the service objects and provides them when requested by a service platform. It plays an essential role in supporting user and service mobility, synchronizing multiple instances of the service objects, and providing access to service creation environments.

A service object is located using the alias address of the user to which it belongs. We use the addressing scheme adopted by the Internet Engineering Task Force's Session Initiation Protocol (SIP),[7] in which users are identified by a structured e-mail-like alias: userName@HomeServer. When a service platform needs to download a user's service object, it uses this structure to locate HomeServer and download the service object of userName.

Obviously, this location mechanism is not valid when the user's alias address is outside the adopted addressing scheme. This is the case for E.164 telephone numbers, which in the Internet do not belong to any domain and therefore have to be translated into meaningful structured aliases. Various standards bodies—in particular, the European Telecommunications Standards Institute (ETSI) Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) technical body and its Working Group IV[8]—are addressing this PSTN/IP integration issue, and we expect to use their results.

The home server is also responsible for synchronizing multiple requests for the same service object (for example, when there is more than one call attempt to the same user). This problem stems from the fact that the same service object can be accessed by different service platforms. It can be solved using a centralized approach (the home server is responsible for synchronization) or a distributed one (the service objects communicate among themselves to avoid inconsistencies).

The home server is also where service objects are created. In the traditional telephony network, terminals provide a very poor interface (an alphanumeric keypad with some extra buttons), and the only way to configure services is to type cumbersome sequences of digits. In our solution, a Web-based service creation environment (SCE) can offer a user-friendly GUI-based service configuration. Mizuno et al. describe a similar approach.[9]

SERVICE PLATFORM

The service platform controls service objects' execution life cycles. Once downloaded from the home server, the objects are executed locally and receive events from the underlying communication stacks.

In Figure 1 the GK platform provides the abstraction layer for events coming from a generic network. This abstraction requires the identification of commonalities between existing and emerging communication paradigms adopted by protocols used in wireless, fixed, and VoIP networks. Observe that virtually all of their functionality can be grouped into three main areas: a *registration* phase during which terminals communicate their presence and related data; an *admission* phase during which they ask for a called party's number translation; and a *call signaling* phase during which entities exchange messages to control the actual communication. This distinction allows us to define a level of abstraction that enables different communication stacks to be combined into a single platform.

The user objects encapsulated in service objects (Figure 1) receive fast-changing user information such as the current user location, the user status (busy, free, in a call setup, and so on), or the status of the calls in which the user is involved.

We categorize service objects into three classes.

- *Installed* service objects are downloaded at registration time. They live in the platform until the user unregisters (Figure 1).
- *Downloaded* service objects are downloaded during a call attempt. They live until the call terminates.
- *Replica* service objects are downloaded when other instances of the same service object are already installed into or downloaded to some other service platforms. They live in the service platform in which they are downloaded until the call terminates.

When a user registers with a local GK, the service platform sends a Notify message to the home server, downloads the appropriate service object, and installs it. The Installed service object gets a copy of the user object (created by the GK as soon as the user registers) and initiates it to receive events from the network via the GK and service platform. The service logic behavior is driven by such events, which carry information about the user status and status of

the possible calls in which the user is involved. Examples of services that can take advantage of this updating process are:

- *International call barring.* When a user tries to place a call, the call request is passed to the service object, which uses its logic and the data stored in the user object to do prechecking and decide whether the call can progress.
- *Presence services.* Once the user registers, the service object forwards the user's location to other applications, which can start prescheduled calls or deliver waiting messages.

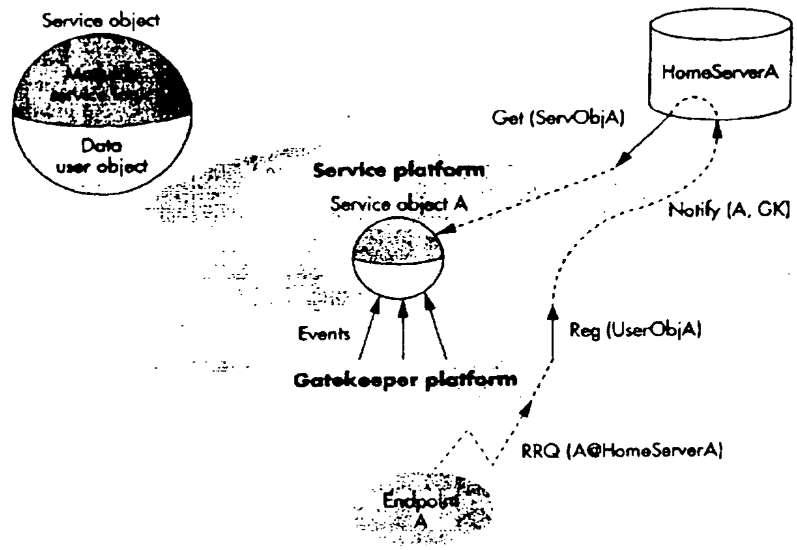


Figure 1. Service architecture (registration time).

When a registered user (for example, user A@HomerServerA in Figure 2) wants to place a call, the GK with which the individual is registered alerts the associated service platform. This platform then checks if the called party's service object is installed locally; if it is not, the appropriate service object is downloaded from the called party's home server. At this stage, two scenarios are possible.

In the first scenario, the called party is registered with a different GK (GK Y in Figure 2). In this case the home server of user B (the called party) creates a called party Replica service object, which contains a reference to the Installed called party service object running in the service platform associated with GK Y. The replica is downloaded into service platform X and retrieves an updated user object from the Installed service object, which is also responsible for the synchronization between itself and its replica.

In the second scenario, the called party is not registered with another GK, so its downloaded service object does not need an updated user object. The called party's status indicates that the user is disconnected. (This is typical when the service logic routes the call to a voice-mail system.) Synchronizing between possible Replica service objects, due to simultaneous call attempts, is left to home server B.

To summarize, the goal is to involve all service objects in a call in the same service platform, which is the one associated with the GK with which the calling party is registered.

An interesting evolution of the proposed architecture is intelligent edge devices running a lightweight version of the service platform. This implies moving it from the service execution layer to the user layer (Figure 2) and removing the GK platform between the device and its service platform. This lets devices access other service platforms directly, avoiding GK mediation.

SERVICE OBJECT BEHAVIOR

Once the service platform has involved all the service objects in the call, the peer-to-peer call negotiation between the objects can start. The calling party's service object invokes a "locate" method (part of the interface of every service object), which chooses the correct destination transport address of the called party. This process could use the user object's fast-changing data.

The service logic implemented by the locate method consists of a set of "if" conditions then actions. The condition field contains information such as time of day, call originator ID, and devices the user is currently using. Possible actions include return transport address, reject, and request further information.

The called party's service object can return a single response or a list of possible options. For example, when the user is unavailable, the calling party's service object can either stop the call or proceed, leaving a message with a voice mail system. When the calling party's service object gets the response, it can execute more logic (address postchecking, availability, and so on) and

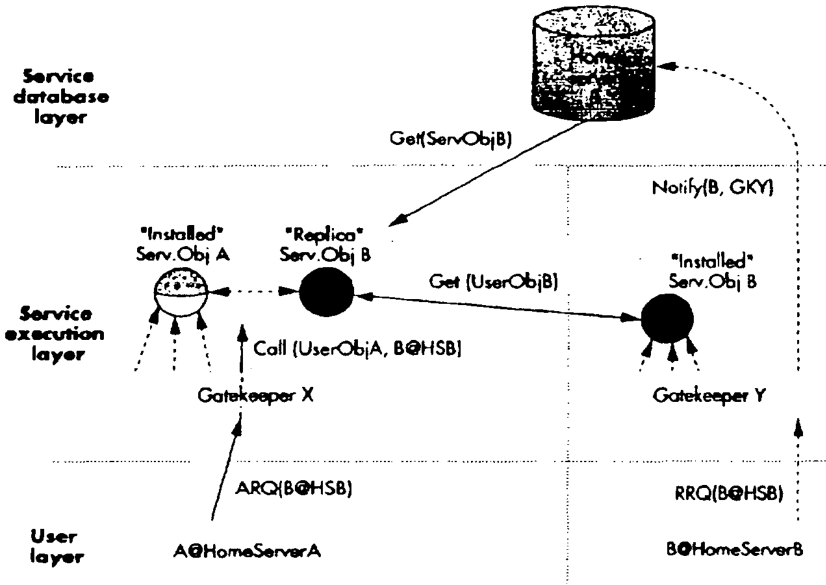


Figure 2. Call placing (from A to B).

then passes the response to the calling party's terminal through the service platform.

For privacy and security reasons, the called party's service object does not have direct access to the calling party's user object. However, it can ask the calling party's service object for information about its user. During this negotiation phase, the two parties agree on the media communication type and format.

As described above, the negotiation phase requires more than a single invocation of the locate method; therefore, it is more reasonable not to call the method remotely on the home server but to transport the whole object through the network.

If $T_{download}$ is the service object downloading time, T_{remote} is the transmission delay for a single message, T_{local} the transmission delay within the platform, and n the number of messages exchanged between the two service objects, the negotiation phase overall delay is $T_1 = T_{download} + 2 * n * T_{local}$ if the whole object is downloaded and $T_2 = 2 * n * T_{remote}$ if it is not. Assuming T_{local} is negligible and $T_{remote} \cong T_{download}$, then $T_1 << T_2$ when n is significantly large. This is the main reason for downloading the called party's service object, even if this could have an impact on postdial delay.

In addition, service mobility has some security implications. Since service objects are downloaded into a foreign service platform, their internal data and methods should not be completely exposed. To overcome this problem, service objects could be implemented as empty proxies and their methods executed via remote calls. This could be a feature home server providers make available. Obviously, security advantages are obtained at the expense of the performance benefits gained by downloading the service objects.

Alternatively, host service platforms have to shield local resources to prevent malicious service objects from accessing local information and communicating relevant data back to the home server or to other applications. This goal can be achieved by using authentication and signed code techniques prior to the execution. Obviously, interoperability between service platforms and home server providers requires well-defined communication interfaces and service-level agreements between them.

PRACTICAL IMPLEMENTATION

Figure 3 (next page) shows the implementation of the service architecture. Because we wanted our prototype to interoperate with currently available VoIP clients, the most popular being Microsoft NetMeeting, we chose H.323 as the VoIP protocol.

The H.323 stack handles messages coming from the IP network. The GK core logic stores information about ongoing calls (call objects) and registered users (user objects) into the respective databases (Figure 3). The components located above the dashed line have been implemented using Java, taking advantage of the built-in remote method invocation (RMI) for communication between these components.

HPLB GATEKEEPER

The HPLB Gatekeeper implements the functionalities described by the H.323 standard except for bandwidth management (Figure 4). Its internal architecture is composed of three functional blocks: the H.323 stack, the interface layer, and the GK, which is divided into the Java communication API and the core logic.

The Java communication API, which sits between the core logic and interface layer, was designed to be independent of the underlying communication protocols. This creates an additional level of abstraction for registration and call admission (RAS) and Q.931 (call signaling). Thanks to

this abstraction a variety of protocols can be plugged into the platform, allowing seamless integration between different networks.

The interface layer between the H.323 stack API, which is written in C, and the Java communication API, is based on the standard Java Native Interface (JNI) mechanism. This layer can be split into two major functions: the message dispatcher and the native methods. The message dispatcher is triggered by callback functions coming from the stack API. It instantiates Java objects with the parameters contained in the received messages and invokes the appropriate communication API methods to pass these objects. Native methods simply map requests from the Java GK logic into H.323 stack API method invocations.

The GK core logic has access to the user and call databases (Figure 4) that contain data related to registered users and ongoing calls, respectively. The user database contains user objects. They contain user status and basic properties such as user alias, E.164 telephone number, and IP address. The status can be DISCONNECTED, REGISTERED, BUSY, or SETUP (if the user is in the call setup phase). The call database contains call objects, consisting of a call-ID, the references of the user objects of all the parties involved in the call, and the call status. The call status reflects the Q.931 messages exchanged between the two endpoints through the GK.

When the GK receives an ARQ, the service platform is invoked to start the service objects' negotiation. After the response is sent back by the service platform and the permission for the call is granted, the Q.931 signaling starts to flow through the GK, updating the related users and call objects. We route H.245 directly between the endpoints because it involves the exchange of a large amount of information of little interest to the GK itself.

The HPLB Gatekeeper core logic implements a simple internal admission policy based on resource availability. Two parameters, based on network capacity, can be set up at launch time: maximum number of registered users and maximum number of ongoing calls. Registrations or call requests that could cause exceeding these parameters are rejected. Future admission policies can be based on more complex interactions with firewalls or bandwidth management servers. These policies could require the interception of the H.245 flow. In fact, if the GK must allocate resources to guarantee QoS for a particular media connection, it should know the UDP port where the stream takes place. The GK can get this parameter by intercepting H.245 messages. This parameter is also useful for monitoring and measurement.

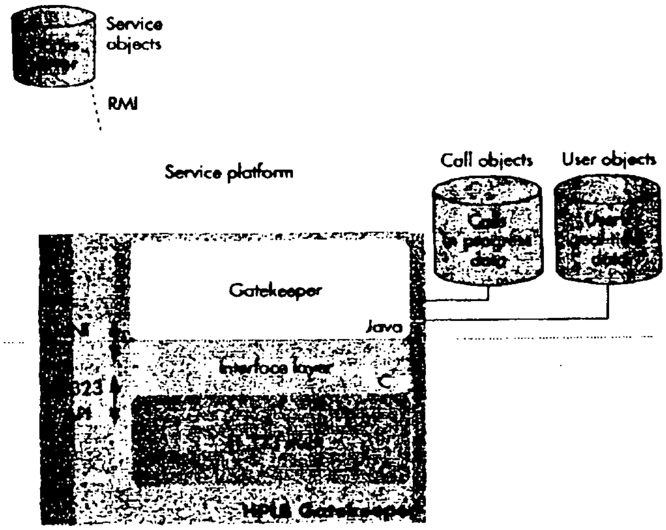


Figure 3. Practical implementation.

SERVICE OBJECTS

Service objects are stored and provided by the home server through the following simple RMI interface:

getServiceObject().
releaseServiceObject().

The mechanism for synchronizing multiple instances of the same service object is implemented within the home server. The service object Java interface is composed of the following methods:

- locate() is invoked by the calling party's service object onto the called party's service object to start call negotiation. In the current implementation this method has one parameter: calling party ID (E.164 number or, preferably, the structured alias when available, that is, when the call comes from an IP terminal).
- die() is used to terminate the object life cycle. Normally, this method is invoked by the service platform when the user unregisters, or by the calling party's object to force stop call negotiation. In the first case, the object is released and the home server notified. In the second case, the behavior is more complicated and depends on whether the object is installed, downloaded, or a replica.
- freeze() is invoked by an installed service object located in the service platform associated with the user's current GK onto a replica of it (Figure

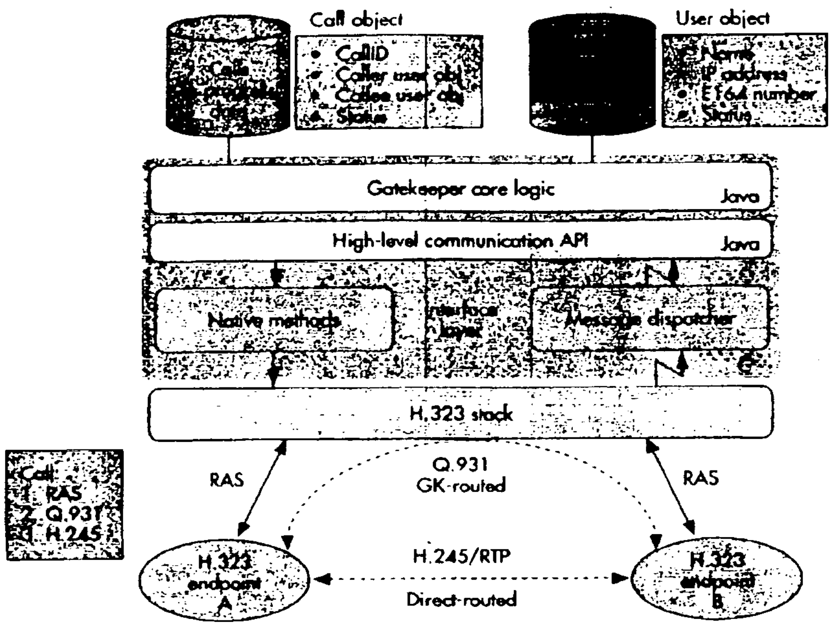


Figure 4. The HPLB Gatekeeper platform.

2). This method is used to temporarily freeze the replica to avoid conflicts between the decisions made by the two objects, which may affect the user.

- unfreeze().
- release() is invoked by a replica service object to notify the original installed object that it no longer exists.
- getUserStatus().
- getServiceStatus(). The service status can be normal or frozen. If a service object is frozen, it is likely that the other party's service object will stop the call.
- updateUserStatus() and updateCallStatus() are invoked by the service platform.

H.323v2 can benefit from the service object negotiation. In fact, its Fast Connect procedure coupled with the prior service object's call negotiation ensures that media channels with the optimal characteristics—chosen during this call negotiation—can be opened just after call setup. This requires passing terminal capabilities to the GK at registration instead of exchanging them during the H.245 phase, after service object negotiation. While this feature is already part of the SIP protocol, H.323 will provide it in future versions. This is one of the problems that must be solved when integrating different protocol stacks under a common level of abstraction.

It is also worth pointing out the relationship between H.450 and our proposal. The former is a signaling mechanism to control services implementation; the latter, the logic behind it.

Since service objects are essentially Java objects, we use Java as the service logic language, with service logic scripts interpreted by the Java Virtual Machine. Thus we do not need a new virtual machine for interpreting a new scripting language.

There are several proposals for a scripting language that handles calls. The most interesting of them, from a VoIP point of view, is the Call Processing Language (CPL)[10] for Internet telephony, under development by the IPTel IETF Working Group (see the article "Programming Internet Telephony Services" in this issue).

The two main objections to using a normal programming language like Java for service setup by end users are that service creation could be difficult, and that common languages are too complex for handling calls. This complexity can easily generate service misbehaviors. These drawbacks can be overcome by using controlled and simple service creation environments. In this context, we are exploring JavaBeans. JavaBeans can be manipulated graphically, which can generate an interesting evolution of the SCE. In fact, home server providers may make available different classes that can be directly customized by end users using JavaBeans. Different classes of services may be offered, from simple static call redirection (to a number decided by the user) to provision of the whole service object by an end user with good programming skills (which actually implements the whole logic).

DEMONSTRATION

The demonstration described here was presented at the Hewlett-Packard Laboratories review in Bristol last summer. Its aim is to show the ease of deploying personalized user services and the potential interaction with IN components, in particular with the service control point (SCP), the platform currently used by telecom operators to offer value-added services.[2]

The architecture, depicted in Figure 5, provides Internet call waiting, allowing users to receive incoming calls through a VoIP gateway when they are connected via dial-up and their telephone line is engaged.

The SCP is simulated by a Java application running on a machine connected to a private branch exchange (PBX), through specialized cards supporting the British signaling standard DPNSS. This "virtual SCP" communicates with the GK through Java RMI, but call requests reach the GK through the same high-level communication API used by the H.323 stack. A plug-in makes the virtual SCP interoperate with the GK through this API. The H.323 gateway runs on a different machine connected to the same PBX. The range of telephone numbers served by the PBX, connected to the normal PSTN, has been split: a subrange for the GW and another subrange for the virtual SCP. Each extension in the SCP subrange corresponds to an Internet call-waiting subscriber.

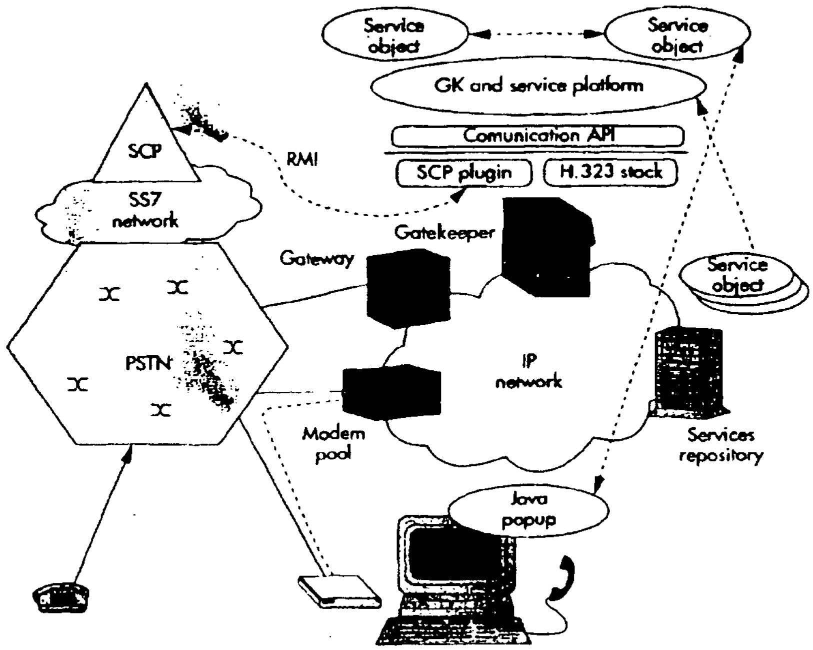


Figure 5. A practical demonstration.

When a call to a subscriber is attempted, the PBX tries to contact the subscriber telephone number. If the number is engaged, the virtual SCP is alerted. The virtual SCP then contacts the GK to find out if the subscriber is registered (note that the user must have registered with the same E.164 number). If so, the process goes on as described: The service platform is invoked and the personalized user service executed.

The demonstration is limited to Internet call waiting, so we assume that whenever the called user is connected via dial-up to an Internet service provider, the user is also registered to the GK associated with the SCP (there is a well-known fixed binding between them). If the called party is not registered to that GK, it means that the user is busy in a PSTN call, and the calling party will get the busy tone (alternatively, the normal IN call-waiting service can be activated).

In our demonstration, the logic in the called party's service object is programmed to examine its own user status. If the user is not busy in a VoIP call, its IP address is returned. Otherwise, the service contacts a small Java application launched at registration running on the current user machine and delivers a popup window, asking the user whether to take the call (leaving to the client the responsibility to manage multiple calls), divert it to another IP address, divert it to a telephone number, or reject it. To do this, the service platform security manager implements a dynamic policy that allows a service object to open a remote connection to the current machine where the registered user is located.

If the user returns an IP address, the GK allocates a "phantom" number on the range associated with the GW. The GK gets this range from the GW at registration through H.323. The GK returns the number to the SCP, keeping the association between the phantom number and the IP address. The virtual SCP communicates with the PBX to divert the incoming call to the GW phantom number. When the GW receives the call, it sends an RAS ARQ message to the GK with the phantom number as destination; the GK knows the IP address associated with that phantom number and connects the H.323 call.

In our demonstration we assume a static relationship between the SCP and the GK-service platform, and every time a user is connected via dial-up to the Internet the user registers with that GK. If the called party can be registered with a GK other than

that associated with the SCP, E.164 number translation is not a trivial task. In particular, the GK associated with the SCP receives, from the SCP, call requests containing just two parameters: caller ID and dialed number. It is important to stress that, in this context, the dialed number is a user identification and not a classic E.164 number. If there are no users registered locally with the E.164 numbers provided by the SCP, the GK must translate E.164 numbers into structured e-mail-like aliases in order to locate the home servers and then download the user objects and service objects. The GK can perform this translation in several ways. It can perform a lookup in a central database or ask other GKs through the Inter-Gatekeeper Communication Protocol (IGCP); see H.323 Annex G.[3]

If the GK can translate these E.164 numbers and locate the called party's and calling party's home servers, service execution proceeds as usual. If not, two scenarios are possible:

- If either the called party's home server is not located or the called party is not registered to any GK, the call is rejected.
- If either the calling party's home server is not located or the calling party is not registered to any GK, a dummy service object is created to interact with the called party's service object.

CONCLUSIONS

VoIP networks have come of age, with significant investment from key industry players. New network and communications technologies are dramatically changing the way services are deployed. There is now a critical need for services that span heterogeneous networks, and VoIP, with its extreme openness, will be a key factor in enabling the communication control convergence. In the VoIP context, using this type of active networking through objects downloadable into gatekeeper-like servers seems to be a reasonable way to address the problem.

The architecture presented in this article is a first step in this direction, and more work in this area is expected in the future. Users, carriers, and equipment vendors must map future service requirements and opportunities into an architecture from which protocols, technologies, and products will be determined. The transition from a closed, circuit-switched, usually monopoly- (or oligopoly-) owned telephone network to a much more open and user-configurable packet network poses many difficulties.

Our experience shows that integration between the control elements of traditional and emerging networks is a powerful tool for rapidly deploying and offering new services. We believe that approaches like ours are suitable for the so-called next-generation service providers and will replace the existing closed solutions. ■

REFERENCES

1. H. Schulzrinne, "Re-engineering the Telephone System," *Proc. IEEE Singapore Int'l Conf. Networks*, Singapore, Apr. 1997.
2. J. Garrahan et al., "Intelligent Network Overview," *IEEE Comm.*, Vol. 31, No. 3, Mar. 1993.
3. ITU-T Rec. H.323, "Visual Telephone Systems and Equipment for Local Area Networks which Provide a Nonguaranteed Quality of Service," Geneva, Switzerland.
4. D. Isenberg, "The Dawn of the Stupid Network," *ACM netWorker*, Vol. 2, No. 1, Feb.–Mar. 1998, pp. 24–31.
5. C. Low, "Integrating Communication Services," *IEEE Comm.*, Vol. 35, No. 6, June 1997.
6. O. Kahane and S. Petrack, "Call Management Agent System Requirements Function Architecture and Protocol," IMTC VoIP Forum, Seattle, Wash., Jan. 1997; work in progress: ftp://ftp.imtc-files.org/imtc-site/VoIP-AG/VoIP97-010.doc.
7. M. Handley, H. Schulzrinne, and E. Schooler, "SIP: Session Initiation Protocol," Internet draft, IETF, Jan. 1999; work in progress.
8. "Telecommunications and Internet Protocol Harmonization Over Networks," TIPHON, http://www.etsi.org/tiphon.
9. O. Mizuno et al., "Advanced Intelligent Network and the Internet Combination Service and Its Customization," *IEICE Trans. Comm.*, Vol. E81B, No. 8, Aug. 1998.
10. J. Lennox and H. Schulzrinne, "Call Processing Language Requirements," Internet draft, Internet Engineering Task Force, July 1998; work in progress.

Daniele Rizzetto is a member of the technical staff at Hewlett-Packard Laboratories, Bristol, UK. He graduated in computer science from the University of Padua, Italy, in 1995, and earned a postgraduate degree in network systems from Cefriel-Politecnico di Milano, Italy, in 1997. He is interested in the impact of Internet telephony on traditional telephony and next-generation service platforms for telecommunications.

Claudio Catania is a senior member of the technical staff at Hewlett-Packard Laboratories, where he focuses on the impact of disruptive technologies on advanced communication services. He received the Laurea degree in electronic engineering from Politecnico di Milano, Italy, in 1995, and a post-graduate specialization degree in information technology from Cefriel (Politecnico di Milano), where he studied mathematical models for performance evaluation of interconnection networks.

Readers can contact Rizzetto at daniele_rizzetto@hp.com and Catania at cld@hpl.hp.com.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 909 064 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.04.1999 Bulletin 1999/15

(51) Int Cl.6: **H04L 12/66**, H04M 7/00, H04Q 3/00

(21) Application number: **98410091.7**

(22) Date of filing: **10.08.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.08.1997 JP 228965/97**

(71) Applicant: **KOKUSAI DENSHIN DENWA CO., LTD**
Shinjuku-ku Tokyo (JP)

(72) Inventors:
- **Oda, Toshikane**
  Fujimi-shi, Saitama (JP)
- **Yamada, Hideaki**
  Itabashi-ku, Tokyo (JP)
- **Yagi, Hikaru**
  Asaka-shi, Saitama (JP)
- **Masaki, Hiroto**
  Katsushika-ku Tokyo (JP)

(74) Representative: **de Beaumont, Michel**
1, rue Champollion
38000 Grenoble (FR)

(54) Routing control communication system between circuit switched network and internet

(57) A routing control communication system includes a circuit switched network provided with a service control information database having a telephone numbers table, an interconnection network provided with a network communication protocol and an information terminal, and a network interworking equipment provided with one terminal connected with the circuit switched network and the other terminal connected with the interconnection network. The information database is connected with the interconnection network, and the information terminal of the interconnection network is constituted so as to obtain a transferred terminal number corresponding to a called telephone number from the service control information database.

Fig. 1A

Fig. 1

Fig. 1A	Fig. 1B

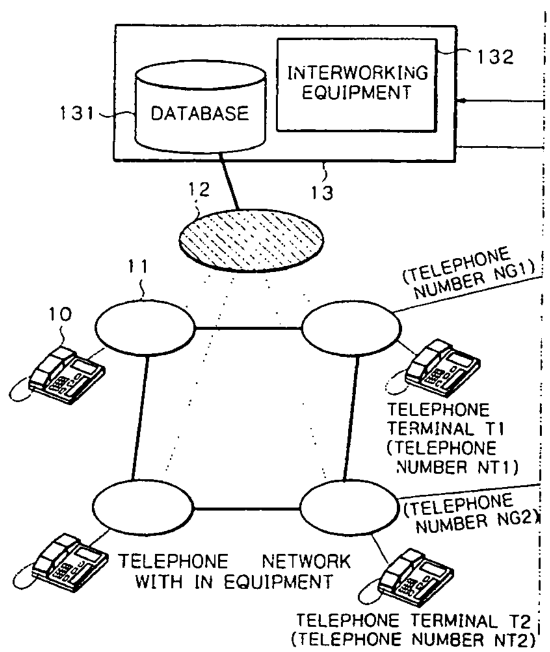
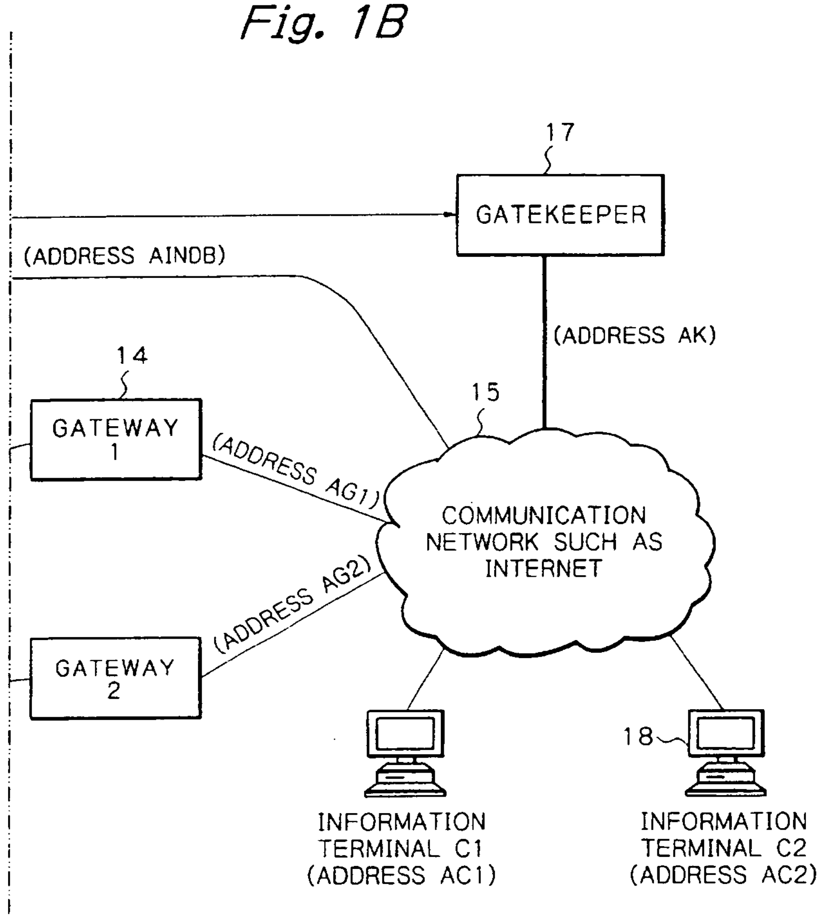


Fig. 1B


17
GATEKEEPER
(ADDRESS AINDB)
(ADDRESS AK)
14
GATEWAY 1
(ADDRESS AG1)
15
COMMUNICATION NETWORK SUCH AS INTERNET
(ADDRESS AG2)
GATEWAY 2
18
INFORMATION TERMINAL C1 (ADDRESS AC1)
INFORMATION TERMINAL C2 (ADDRESS AC2)

Description

FIELD OF THE INVENTION

[0001] The present invention relates to a communication system performing routing control between circuit switched network and interconnection network comprising protocol for network communication.

DESCRIPTION OF THE RELATED ART

[0002] ITU-T Recommendation H.323 may be utilized as a protocol for call control in an interconnection network (hereinafter called as internet) having network communication protocol like LAN, WAN or the Internet based on the IP networking technique. H.323 includes Q.931 protocol which is used as a call control signaling for establishing and releasing calls among terminal equipment and gateways in the internet, where the gateway is an equipment which interconnects between a call in the circuit switched network such as telephone networks, integrated services digital networks and mobile communication networks and a call in the internet. The network architecture in the H.323 includes a gatekeeper which performs functions of address translation. access control, bandwidth management, etc. The gatekeeper may have additional functions relating to the call control such as a conference call control.

[0003] In many cases, a public switched telephone network is constructed as Intelligent Network (IN) in order to provide enhanced and diversified network service. The IN is a network connection architecture recommended in Q. 1200 series of ITU-T. Difference between conventional network and the IN are two points of independence and integration of the service control function from the switching equipment.

[0004] An aim of the conventional telephone switching system is to efficiently provide one to one communication services. However, in order to provide the service control function to each switching equipment, complex addition and modification on the function are required. Therefore, advancing of services is somewhat limited. The IN solves this problem by constructing a layered structure such that the switching equipment executes a basic call connection function and a dedicated information processing equipment executes a function for providing complex services. According to the IN, a service control function needed for realization, maintenance and operation of the network services is integrated and controlling, monitoring and managing of the call control part are performed so as to meet an introduction of advanced network services. Additional services such as freephone service, abbreviated dialing service, virtual private network service and transfer service are realized with the IN technique.

[0005] A part of structure of IN can be seen in Fig. 1. In the figure, a call control part 11 for performing only basic connection of a circuit such as a digital switching system, a service control part 12 for directing the service to the call control part 11, and a service control information database 13 for storing service control information are illustrated.

[0006] In a PBX and a private communication network composed mainly with dedicated line, these additional services are realized by adding a service control function to a server equipment connected to the PBX.

[0007] However, when a call for connecting to a telephone terminal in a telephone network is originated from an information terminal of the internet, it is not sure that the nearest gateway with respect to the called telephone terminal is always selected. The longer in distance between a selected gateway and the called telephone terminal, the less efficient use of communication resources due to wasteful routing. This invites an inconvenience to users in paying increased charge to the telephone networks.

[0008] Hitherto, the internet provides gatekeeper. When a call from an information terminal C1 of the internet to a telephone terminal T1 of the telephone network is arrived, the information terminal C1 inquires to the gatekeeper and thus the gatekeeper responds by retrieving a gateway address AG1 for the called telephone number NT1. Therefore, the gatekeeper has an address table to take the correspondence between the telephone number and the address of the gateway used to connect to the telephone number. The routing control can be thus performed by selecting the address of nearest gateway depending upon the called telephone number informed from the calling information terminal. However, for the Internet continuing self-increase, it is difficult to always renew the correspondence information in the gateway between the address of the gateway and the telephone number. Therefore, the inconvenience comes out from that communication resources cannot use efficiently for wasteful routing as mentioned above.

[0009] More concretely, an inconvenience may come out in case of usage of the call transfer service. For example, it is assumed that there is a service for transferring a calling to a telephone terminal T1 of the telephone network to an information terminal C2 of the internet is set, and that an information terminal C1 of the internet originates a call to the same telephone terminal T1 of the telephone network through the gateway. In this case, the service control part of the telephone switching system, which detects that the telephone terminal T1 is called. needs to execute a procedure for terminating the call to the information terminal C2 by transferring again the call into the internet through the gateway. Such wasteful procedure between the networks will produce further consumption of the communication resources. This problem is caused by that the one communication network has only information for call transfer to the other communication network. The similar problem will occur in case that a mobile terminal equipment to be called in the

Q2(3) [first information part] = Called telephone number.

[0033] In case that a signal is directly sent to a service control part of the IN facility, a signal with a signal format depending on the Intelligent Network Application Protocol (INAP) and communication with the procedure of the INAP is executed, or a signal with a signal format depending on the Transaction Capabilities Application Part (TCAP) and communication with the procedure of the INAP is executed. On the other hand, it enables to communicate with existence communication procedures different from these ones. The signal Q2 composed like this is sent to an IN facility signal transmission unit 205 and outputted to the service control information database in the IN facility.

[0034] At this time, the internet signal analyzing unit 207 sends the received inquiring signal Q1 to a signal corresponding management unit 210, and the signal corresponding management unit 210 memorizes in a memory 212 for the advising contents.

[0035] The service control information database retrieves the called telephone number T1 for the inquiring signal Q2, and sends the response signal R1 provided with retrieved transferred terminal number to the interworking equipment 132. The transferred terminal number is the telephone number in case of telephone network, or is an address in case of the internet.

[0036] - An IN facility signal receiving unit 201 of the interworking equipment 132 receives the response signal R1 from IN facility and sends it to an IN facility signal analyzing unit 202. The IN facility signal analyzing unit 202 analyses contents of response signal R1. At this time, by inquiring to the signal corresponding management unit 210 to obtain a reference number and by comparing the obtained reference number with a reference number in the responding signal R1, it is confirmed that the responding signal R1 is a corresponding response to the inquiring signal Q1. After the confirmation, the IN facility signal analyzing unit 202, in order to advice the signal R2 as the response information for the gatekeeper, forms the response information in the signal formats as follows:

R2(1) = Q1(1),
R2(2) = Telephone number conversion response,
R2(3) = Called telephone number,
R2(4) = Transferring terminal number.

The unit 202 sends these response signal R2 to an internet signal assembling unit 203.

[0037] The Internet signal assembling unit 203 composes the response signal R2 to be sent to the gatekeeper and sends it to an internet signal transmission unit 204. The internet signal transmission unit 204 sends a received response signal R2 to the gatekeeper.

[0038] The gatekeeper 17, that receives the response signal R2, obtains transferred terminal number. In case that there is difference between the called telephone number and transferred terminal number, the gatekeeper 17 retrieves an address table based on this transferred telephone number. The gatekeeper 17 obtains an address of the gateway, if the transferred terminal number would be the telephone number. After that, the gatekeeper 17 sends the obtained address to the calling information terminal C1.

[0039] The service database equipment 13 of the IN facility can connect to the internet with an address AINDB. As a result. The equipment 13 can perform accessing from, not only the gatekeeper 17 but also any all information terminals in the internet. In moreover, the equipment 13 enables to compose such as the cache for corresponding table with the called telephone number obtained and the transferred terminal number.

[0040] Hereinafter, from the point of view of total communications, the sequence will be explained at case of calling from the information terminal C1 of the internet. information terminal C1 inquires the telephone number or the address as the called terminal number for the gatekeeper 17. If it is judged in the gatekeeper 17 that the called terminal number is the telephone number, it inquires within the service database equipment 13 by including previously mentioned inquiring signal Q1 with the called telephone number. From the responding signal R2, a transferred terminal number corresponding to the called telephone number can be obtained. For instance, if it would be settled in the service control information database 131 that the call to the telephone terminal T1 is to transfer to information terminal C2, the address of the information terminal C2 is included in the responding signal as the transferred terminal number. The gatekeeper 17 which received the responding signal can advice the transferred address to the information terminal C1. If it is settled in the service control information database 131 so that the call to the telephone terminal T1 is to transfer to the telephone terminal T2, the telephone number of the telephone terminal T2 is included in the responding signal as the transferred terminal number.

[0041] The similar functions are needed in case of call connection in which called telephone number is converted as in freephone service and VPN service. That is, in case that practical called terminal is to be identified with the internet address as information terminal C1, an originating switching equipment has to obtain a telephone number of the gateway for information terminal C1 to be identified with transferred address.

[0042] If there are requirement conditions for setting that a communication route through the internet is to be modified

by quality or else, it is needed to have a function to select optimum gateway from the internet address.

(2) In case that the service database of IN facility obtains transferred gateway telephone number group corresponding called address from the gatekeeper.

[0043] Fig. 2 shows that, in the interworking equipment 132, the inquiring signal F1 provided with a transferred address is inputted from the IN facility and its conversion signal F2 is outputted for the gatekeeper. Also, the response signal G1 for the inquiring signal F1 is inputted from the IN facility and its conversion signal G2 is outputted for the IN facility.

[0044] The service control part 12 of the IN facility which receives an inquiry relating to called telephone number X1 from the switching equipment generating a call obtains the transferred address Y1 of the called telephone number from the record in the service control information database 131. The service control part 12 composes the inquiring signal F1 for the gateway telephone number including address Y1, and sends the signal F1 to the interworking equipment 132.

[0045] The inquiring signal F1 is received with the IN facility signal receiving unit 201 in the interworking equipment 132. The signal receiving unit 201 sends the inquiring signal F1 for the IN facility signal analyzing unit 202. The signal analyzing unit 202 analyzes the contents of the signal F1, and then discriminate its inquiring contents. The signal analyzing unit 202, moreover, composes the inquiring signal F2 of the gateway telephone number to the address Y1 for the gatekeeper of the internet indicating the internet signal assembling unit 203.

[0046] The assembling unit 203 composes of the following inquiring signal F2:

F2(1) = reference number,
F2(2) = gateway telephone number inquiring,
F2(3) = transferred address Y1.

The signal F2 is transmitted to the internet signal transmission unit 204, and is outputted to the gatekeeper 17.

[0047] The gatekeeper 17 identifies that it should be inquiry about the gateway telephone number from the discriminating code of F2(2) when receiving the inquiring signal F2.

[0048] The gatekeeper 17 has the correspondence table between the address and the gateway telephone number. The correspondence table is administrated within the internet, and the correspondence between the address and the gateway telephone number is used to modify properly depending upon the internal status of the internet, network topology and circuit bandwidth. The gatekeeper 17 then retrieves the contents of the correspondence table with the inquiry signal F2 and obtains the gateway telephone number Z1(m) corresponding with the address Y1. The gateway telephone number Z1(1, 2, . . . , M) includes plural gateway telephone numbers and hereupon, Zl(m) shows mth candidate for telephone number.

[0049] The gatekeeper sends obtained gateway telephone number group Z1(1, 2, . . , M) to the interworking equipment 132. The response signal G1 are composed as following:

G1(1) = reference number,
G1(2) = gateway telephone number corresponding,
G1(3) = address Y1,
G1(4) = obtained gateway telephone number group Z1(1, 2, . . . , M)

[0050] The response signal G1 from the gatekeeper 17 is received at the internet signal receiving unit 208 of the interworking equipment 132, and is transmitted to the internet signal analyzing unit 207. The signal analyzing unit 207 analyzes the contents of the received response signal G1, obtains reference number with inquiring for the signal correspondent administration unit 210, compares the obtained reference number with reference number included in the response signal G1, and confirms to be corresponding response to the inquiring signal F1. After that, the unit 207 discriminates to be the response for inquiry from the identifying code of G1(2). Then, in order to notify to the IN facility of inquiring source the contents, obtained gateway telephone number group Z1(1, 2, . . , M), responding to the inquiring signal F1, it directs to the IN facility signal transmission unit 205 so as to compose a signal G2 and to transmit the composed signal G2.

[0051] The signal transmission unit 205 sends the response signal G2 including the gateway telephone number group Z1(1, 2, . . . , M) to the IN facility.

[0052] The IN facility receives the response signal G2 and it obtains the gateway telephone number group Z1(1, 2, . . , M) for the address Y1 from its contents. In a consequence, the IN facility recognizes the gateway group to be connected, and informs to the generating source switching equipment for the gateway telephone number group Z1(1, 2, . . . , M) or the one of the gateway telephone number Z1(m) and address Y1.

[0053] The generating source switching equipment, at receiving this information, selects the one from received gateway telephone number group Z1(1, 2, . . . , M), and together with proceeding the arrange for connecting to the gateway of its number, the address Y1 of called terminal is informed to the gateway with indicating on the information element

of the call connection control signal.

[0054] The gateway which has received the call connection signal for a call, reads out the address Y1 of called terminal indicating on the information element of the call connection control signal, and connects the call to the called terminal of the internet.

[0055] In the above-mentioned procedure, the call connection based on the called number X1 of the call completes at all. The gateway corresponding first number Z1(1) of the gateway telephone number group Z1(1, 2, . . . , M) is nearest gateway for called terminal on the transmission delay within the internet. Thus, if the calling source switching equipment would be set such as to select its gateway in priority, it should be enable to select in automatically a connection route with the smallest signal delay in the internet.

[0056] In the above-mentioned embodiment, described is in case of using the IN facility. However, it is possible to inquire, by the similar protocol as mentioned above, a called telephone number T3 to the database equipment of some specified private communication network. in this case, the IN facility signal assembling unit 206, the IN facility signal transmission unit 205 and the IN facility signal receiving unit 201 should possess functions of transmitting / receiving of an information depending on the communication procedure to communicate with the database equipment in the private communication network.

[0057] If the called telephone number T1 is a number using freephone service and the transferred telephone number T2 which is obtained by using the IN facility is the terminal logic number registered in the mobile communication network, the interworking equipment 132 according to the present invention inquires the transferred telephone number T2 to the number conversion database equipment of the home mobile communication network so that the called terminal inquires for the transferred telephone number T3 to the roaming mobile communication network.

[0058] In this case, the interworking equipment 132 according to the present invention holds the telephone number classified information table, as shown in Table 1, in the number information memory 211.

Table 1

NUMBER CLASSIFICATION	SERVICE CLASSIFICATION
0 1 2 0 x x x x x x	FREEPHONE SERVICE NUMBER
0 9 9 0 x x x x x x	INFORMATION SERVICE NUMBER
0 3 0 x x x x x x x	MOBILE COMMUNICATION NETWORK SUBSCRIBER'S NUMBER
. . .	. . .

[0059] The IN facility signal analyzing unit 202, when obtaining the transferred telephone number T2, refers the telephone number classified information table in the number information memory, and checks that [the called number T1 is equal to the number using freephone service] and [the transferred telephone number T2 is equal to the terminal logic telephone number registered in mobile communication network]. The IN facility signal analyzing unit 202, when it is judged that the above-mentioned conditions are satisfied, directs to the internal signal assembling unit 209 to execute process of the inquiry again. The directed signal assembling unit 209 composes new inquiry signal Q3 as follows;

Q3(1) = the reference number,
Q3(2) = telephone number inquiry,
Q3(3) = transferred telephone number T2.

Then, the signal assembling unit 209 transmits an inquiry signal Q3 to the internet signal receiving unit 208. Thus, the aforementioned protocol for telephone number conversion is executed so that the interworking equipment 132 obtains new transferred telephone number T3.

[0060] In case that the interworking equipment according to the present invention is realized in the gatekeeper, it is possible to use the bus in the gatekeeper equipment.

[0061] According to the present invention, it is possible to efficiently use communication resources at setting up the route of the call connection between the interconnection network having network communication protocol and circuit switched network. For instance, it is possible to inquire to the service control information database of the IN facility, whether there is a transferred terminal number for called telephone number or not. In case that the transferred terminal number is the telephone number, it is possible to transfer for telephone number of optimum gateway. If transferred terminal number is an address of a interconnection network, it is possible to call directly for prescribed address. In

short, it is not to pay for useless commúnication cost.

[0062] If the gatekeeper having address table is connected with the internet, it is possible to embody the routing control of communication systems using communication resources efficiently by mutual communicating with service control information database provided with telephone number table. It is not necessary to administrate for network information of each other, by performing of inquiry / response for table information with between both, and then it is not needs for complexity of communication systems. Also, for a role of protocol conversion on the service control information database and the gatekeeper, it is possible to use for existing IN facility and the gatekeeper. Besides, as the transferred gateway in communications, it is possible to select the available gateway for the route of quality agreed with needs of communication user for called terminal and communication route.

[0063] The network routing control communication systems according to the present invention with special structure mentioned above can offer special effects for communication enterpriser, service provider and user.

[0064] Many widely different embodiments of the present invention may be constructed without departing from the spirit and scope of the present invention. It should be understood that the present invention is not limited to the specific embodiments described in the specification, except as defined in the appended claims.

Claims

1. A routing control communication system comprising:

    a circuit switched network provided with a service control information database having a telephone numbers table:
    an interconnection network provided with a network communication protocol and an information terminal; and
    a network interworking equipment provided with one terminal connected with said circuit switched network and the other terminal connected with said interconnection network,
    said information database being connected with said interconnection network, and the information terminal of said interconnection network being constituted so as to obtain a transferred terminal number corresponding to a called telephone number from said service control information database.

2. The system as claimed in claim 1, wherein said information terminal of said interconnection network for obtaining the terminal number to be transferred includes a memory means for storing relationship information between said obtained called telephone number and the transferred terminal number.

3. The system as claimed in claim 1, wherein said transferred terminal number identifies a telephone number of a circuit switched network.

4. The system as claimed in claim 1, wherein said transferred terminal number identifies an address of said interconnection network.

5. The system as claimed in claim 1, wherein the information terminal of said interconnection network for obtaining the transferred terminal number is a gatekeeper having an address table of said interconnection network, and wherein said service control information database is constituted so as to obtain from said gatekeeper a telephone number of a transferred gateway which corresponds to a called address.

6. The system as claimed in claim 5, wherein a plurality of gateway telephone numbers to be transferred are obtained from said gatekeeper, simultaneously.

7. The system as claimed in claim 1, wherein a interworking equipment is connected to said service control information database, and wherein the interworking equipment performs mutual signal exchange for enquiry / response signals.

8. The system as claimed in claim 7, wherein said interworking equipment includes a memory means for storing information relating to mutual signal exchange of enquiry / response signals.

9. The system as claimed in claim 1, wherein said circuit switched network includes an IN.

10. The system as claimed in claim 1, said network interworking equipment is a gateway.

Fig. 1A

Fig. 1

Fig. 1A	Fig. 1B

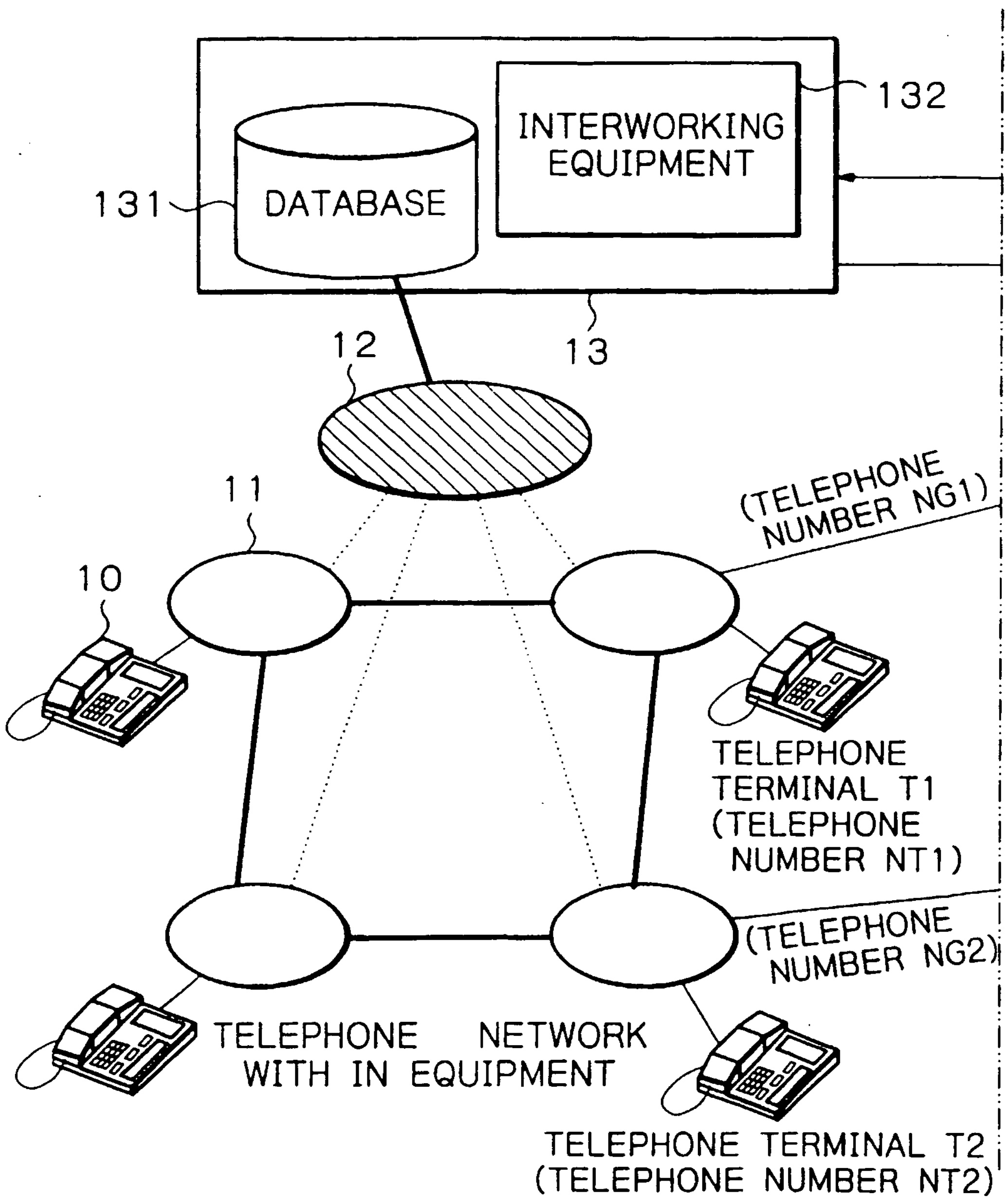


Fig. 1B

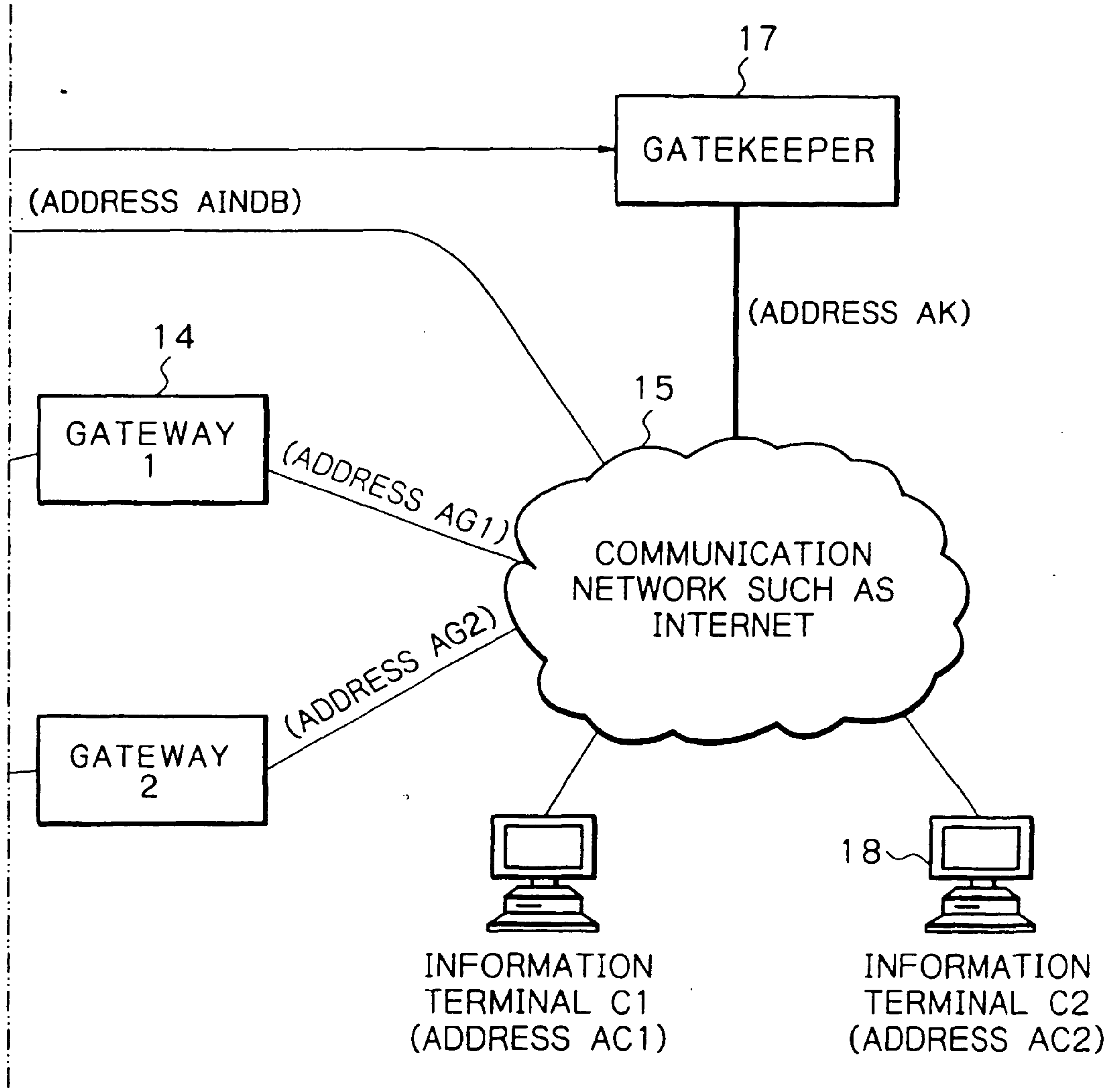

17
GATEKEEPER
(ADDRESS AINDB)
(ADDRESS AK)
14
15
GATEWAY
1
(ADDRESS AG1)
COMMUNICATION
NETWORK SUCH AS
INTERNET
(ADDRESS AG2)
GATEWAY
2
18
INFORMATION
TERMINAL C1
(ADDRESS AC1)
INFORMATION
TERMINAL C2
(ADDRESS AC2)

Fig. 2

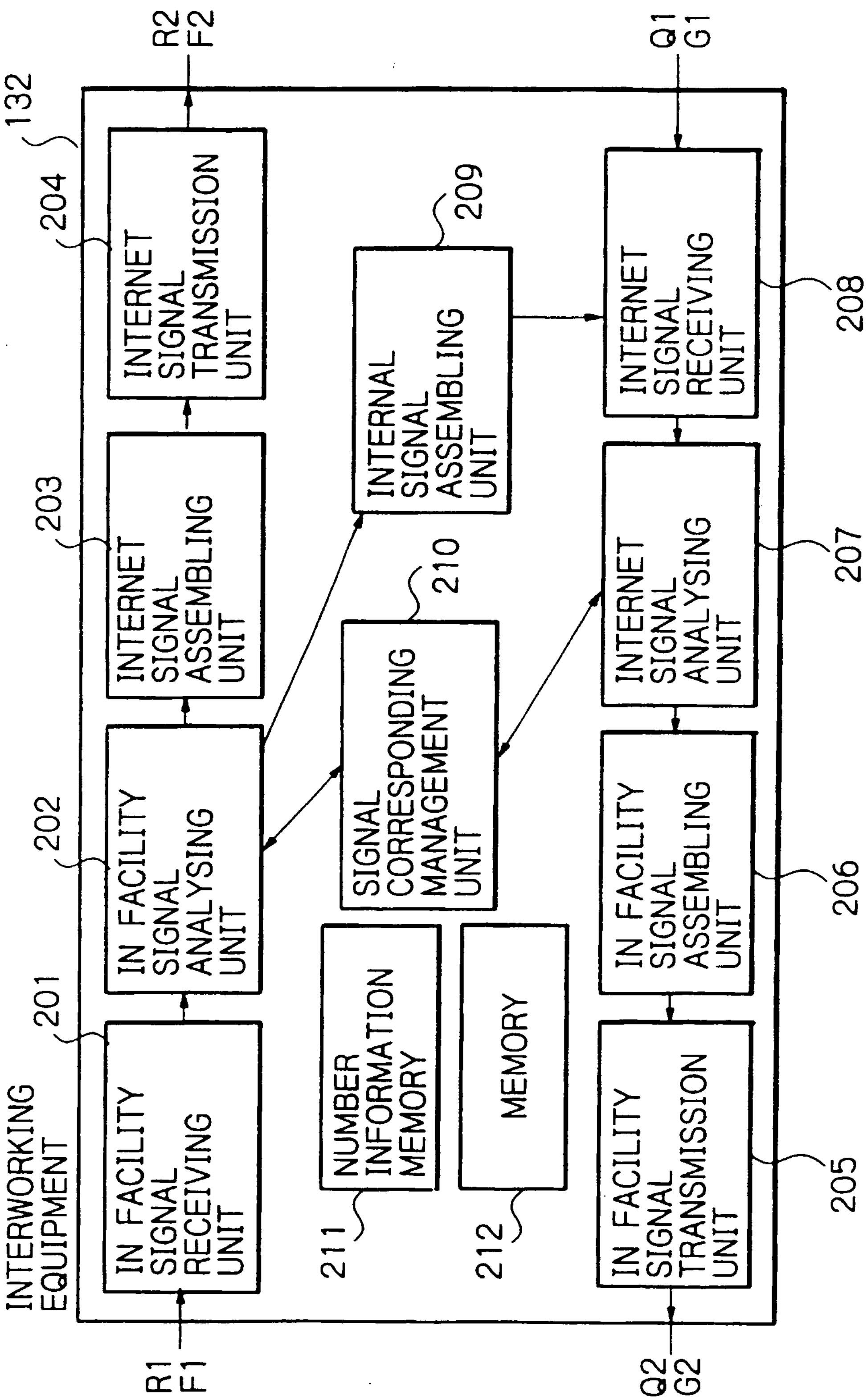

INTERWORKING EQUIPMENT
132
R1
F1
R2
F2
Q1
G1
Q2
G2
201
IN FACILITY SIGNAL RECEIVING UNIT
202
IN FACILITY SIGNAL ANALYSING UNIT
203
INTERNET SIGNAL ASSEMBLING UNIT
204
INTERNET SIGNAL TRANSMISSION UNIT
209
INTERNAL SIGNAL ASSEMBLING UNIT
210
SIGNAL CORRESPONDING MANAGEMENT UNIT
211
NUMBER INFORMATION MEMORY
212
MEMORY
208
INTERNET SIGNAL RECEIVING UNIT
207
INTERNET SIGNAL ANALYSING UNIT
206
IN FACILITY SIGNAL ASSEMBLING UNIT
205
IN FACILITY SIGNAL TRANSMISSION UNIT

Fig. 3

REFERENCE NUMBER	CLASSIFICATION CODE	FIRST INFORMATION PART	SECOND INFORMATION PART		Nth INFORMATION PART
S (1)	S (2)	S (3)	S (4)	....	S (N-2)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 909 064 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.09.1999 Bulletin 1999/35

(51) Int Cl.6: H04L 12/66, H04M 7/00, H04Q 3/00, H04L 29/06

(43) Date of publication A2:
14.04.1999 Bulletin 1999/15

(21) Application number: 98410091.7

(22) Date of filing: 10.08.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 12.08.1997 JP 22896597

(71) Applicant: KOKUSAI DENSHIN DENWA CO., LTD
Shinjuku-ku Tokyo (JP)

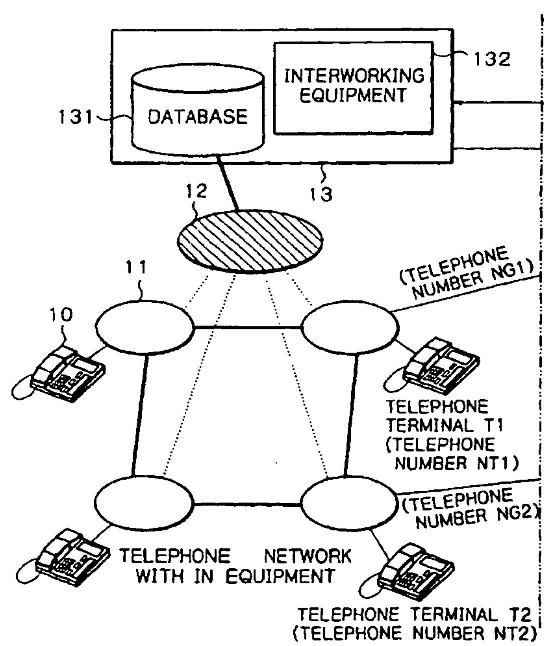
(72) Inventors:
- Oda, Toshikane
Fujimi-shi, Saitama (JP)
- Yamada, Hideaki
Itabashi-ku, Tokyo (JP)
- Yagi, Hikaru
Asaka-shi, Saitama (JP)
- Masaki, Hiroto
Katsushika-ku Tokyo (JP)

(74) Representative: de Beaumont, Michel
1, rue Champollion
38000 Grenoble (FR)

(54) Routing control communication system between circuit switched network and internet

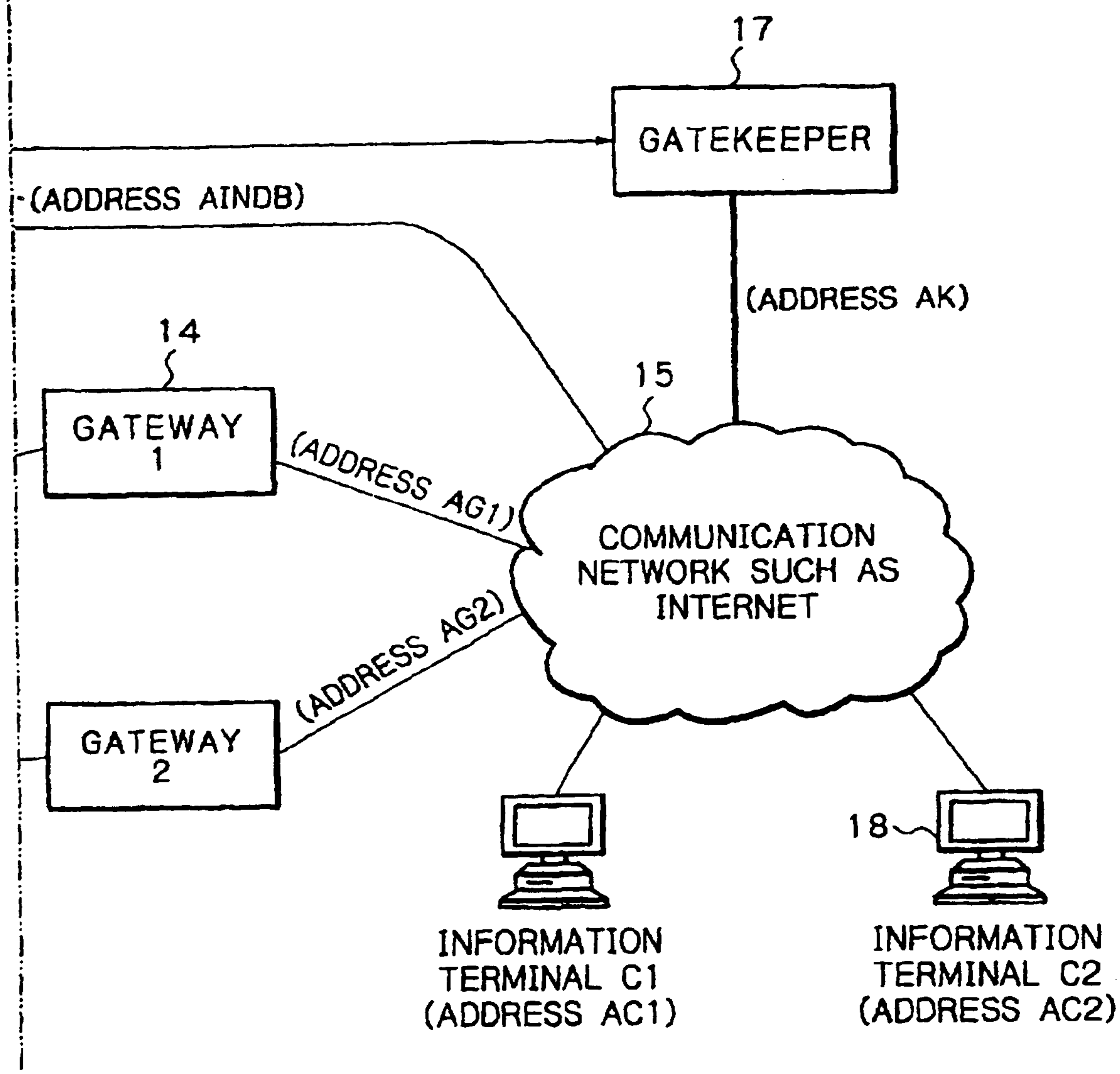
(57) A routing control communication system includes a circuit switched network (12) provided with a service control information database (131) having a telephone numbers table, an interconnection network (15) provided with a network communication protocol and an information terminal (18), and a network interworking equipment provided with one terminal connected with the circuit switched network (132) and the other terminal connected with the interconnection network (17). The information database (131) is connected with the interconnection network (15), and the information terminal (18) of the interconnection network is constituted so as to obtain a transferred terminal number corresponding to a called telephone number from the service control information database (131).

Fig. 1A



EP 0 909 064 A3

Fig. 1B


17
GATEKEEPER
(ADDRESS AINDB)
(ADDRESS AK)
14
GATEWAY 1
15
(ADDRESS AG1)
COMMUNICATION NETWORK SUCH AS INTERNET
(ADDRESS AG2)
GATEWAY 2
18
INFORMATION TERMINAL C1 (ADDRESS AC1)
INFORMATION TERMINAL C2 (ADDRESS AC2)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 41 0091

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	WO 97 16007 A (SAKSANEN PAULI ;FINLAND TELECOM OY (FI); KARHAPAEAE TUOMO (FI)) 1 May 1997 * page 4, line 1 - line 23 * * page 5, line 4 - line 12 * * page 5, line 22 - page 6, line 5 * * page 7, line 9 - line 31 * * page 11, line 7 - line 10 * ---	1,3,4, 7-10	H04L12/66 H04M7/00 H04Q3/00 H04L29/06
A	WO 96 38018 A (KOPONEN HARRI ;KAAKKOLA MATTI (FI); MELEN BJOERN (FI); VAEAENAENEN) 28 November 1996 * page 4, line 13 - page 5, line 9 * * page 9, line 8 - line 15 * * page 13, line 1 - line 5 * ---	1,3,4,9, 10	
A	WO 97 14238 A (INT DISCOUNT TELECOMMUNICATION) 17 April 1997 * page 3, line 28 - line 39 * * page 4, line 36 - page 5, line 2 * * page 6, line 12 - line 22 * * page 11, line 24 - line 39 * -----	1,3,4,10	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L H04Q H04M

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 June 1999	Brichau, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 41 0091

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-06-1999

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9716007	A	01-05-1997	AU	7302596 A	15-05-1997
			FI	955810 A	26-04-1997
WO 9638018	A	28-11-1996	FI	961690 A	25-11-1996
			AU	5916696 A	11-12-1996
			CA	2221183 A	28-11-1996
			CN	1185268 A	17-06-1998
			EP	0829181 A	18-03-1998
			NO	975343 A	21-01-1998
WO 9714238	A	17-04-1997	EP	0855114 A	29-07-1998
			LV	12247 A	20-03-1999
			NO	981540 A	12-06-1998
			PL	327401 A	07-12-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82